

Adversary lower bounds in the Hamiltonian oracle model *

David Yonge-Mallo

Abstract

In this note, we show that quantum lower bounds obtained using the adversary method hold in the Hamiltonian oracle model.

1 Introduction

The adversary method is one of the two main techniques for proving lower bounds in the quantum query model (the other being the *polynomial method*). It is an extremely versatile method with several equivalent formulations which has been used to obtain good lower bounds for a variety of functions. It can be understood in terms of weight schemes [Amb06, Zha05], via semidefinite programming and spectral analysis [BSS03], or through Kolmogorov complexity [LM03]. All of these formulations have been shown to be equal both in their power and in their limitations [SS06]. Later, an extension of the adversary method was introduced which allows the use of negative weights and removes some of the limitations of the method [HLS07].

2 Discrete oracles, fractional oracles, and Hamiltonian oracles

Suppose that we wish to compute some function $f : \{0,1\}^N \mapsto \{0,1\}$, given the input variables $x = x_1x_2 \cdots x_N$, using a quantum algorithm. The state of the algorithm at any time t , on the input string x , may be written in terms of a set of basis states $|j, k\rangle$ such that the first $\lceil \log N \rceil$ qubits j range over the indices of the variables:

$$|\psi_x^t\rangle = \sum_{j,k} \alpha_{j,k} |j, k\rangle$$

In the conventional (*discrete*) *quantum query model*, access to the variables is allowed only through a discrete oracle, which can be queried with index j to obtain the value of the variable x_j . The query complexity of any particular algorithm computing f is the number of queries made by that algorithm, and the query complexity of the function f itself is the minimum query complexity of any algorithm computing f . In this model, we typically¹ define the query transformation Q_x so that the basis state $|j, k\rangle$ queries the variable x_j , and gains a negative phase if $x_j = 1$. Then the query maps $|j, k\rangle$ to $(-1)^{x_j} |j, k\rangle$, that is,

$$Q_x |j, k\rangle = \begin{cases} |j, k\rangle & \text{if } x_j = 0, \\ -|j, k\rangle & \text{if } x_j = 1. \end{cases}$$

In addition to queries, a discrete quantum query algorithm can also perform arbitrary unitary transformations that do not depend on the input string x . An algorithm that makes T discrete queries (T is an integer) is just a sequence of operations alternating between arbitrary unitary transformations and queries:

$$U_0, Q_x, U_1, Q_x, U_2, Q_x, \dots, Q_x, U_{T-1}, Q_x, U_T$$

*This manuscript was written in 2007. The section on generalising to negative weights was added in 2011 at the suggestion of Troy Lee.

¹We could also have defined the query so that it maps a basis state $|j, b, k\rangle$ to $|j, b \oplus x_j, k\rangle$. The two formulations are essentially equivalent.

The sequence is applied to the initial state $|\psi^0\rangle$ (which is independent of the input x) to produce the final state $|\psi_x^T\rangle$, which is measured by the algorithm to produce the output. If the output is correct with probability at least $\frac{2}{3}$, we say that the algorithm computes f with bounded error.

The *fractional quantum query model* generalizes the discrete model by allowing fractions of an oracle query to be made. For integer M , the fractional query $Q_x^{1/M}$ maps $|j, k\rangle$ to $(e^{-i\pi/M})^{x_j} |j, k\rangle$. An algorithm in this model is a sequence of operations alternating between arbitrary unitary transformations and such fractional queries:

$$U_{0/M}, Q_x^{1/M}, U_{1/M}, Q_x^{1/M}, U_{2/M}, Q_x^{1/M}, \dots, Q_x^{1/M}, U_{T-1/M}, Q_x^{1/M}, U_T$$

The *Hamiltonian oracle model*, introduced in [FG98], results from taking the limit $M \rightarrow \infty$ in the fractional query model. It is thus a continuous-time generalization of the discrete query model (see [Moc07, FGG07]). In this model, the state of a quantum algorithm $|\psi_x^t\rangle$ evolves according to the Schrödinger equation

$$i \frac{d}{dt} |\psi_x^t\rangle = H_x(t) |\psi_x^t\rangle$$

where $H_x(t)$ is the Hamiltonian of the algorithm. The algorithm starts in the initial state $|\psi^0\rangle$ and evolves for a time T to reach the final state $|\psi_x^T\rangle$. The query complexity of a function f is then the minimum time T needed to compute f .

The Hamiltonian $H_x(t)$ may be decomposed into two parts, a Hamiltonian oracle $H_Q(x)$ that depends on the input string x but is independent of time, and a driver Hamiltonian $H_D(t)$ that depends on the time t but is independent of the input. (Thus, the Hamiltonian oracle corresponds to the oracles calls and the driver Hamiltonian corresponds to the arbitrary unitary transformations in the discrete query model.) To be as general as possible, we can write the combined Hamiltonian, on the input string x , as

$$H_x(t) = g(t)H_Q(x) + H_D(t)$$

for some $|g(t)| \leq 1$.

The Hamiltonian oracle $H_Q(x)$ has the form

$$H_Q(x) = \sum_{j=1}^N H_j(x)$$

where each H_j operates on an orthogonal subspace V_j . That is, writing P_j as the projection onto V_j , we have $H_j = P_j H_j P_j$. We also assume that $\|H_j\| \leq 1$. For each j , there are two possible operators $H_j^{(x_j)}$, corresponding to $x_j = 0$ and $x_j = 1$.

To simulate the fractional or discrete query model using the Hamiltonian query model, let H_j be the matrix with $\pi \cdot x_j$ in the j -th row and column, and zeroes elsewhere. Then each H_j operates on an orthogonal subspace. Note that $H_Q(x)$ is simply the matrix with the string x on the first N entries of the diagonal, multiplied by π , and zeroes everywhere else. If we now choose $g(t) = 1$ and $H_D(t) = 0$ and evolve the basis state $|j, k\rangle$ for a time $1/M$, the result will be the state $(e^{-i\pi/M})^{x_j} |j, k\rangle$, which simulates an oracle call. Likewise, an arbitrary unitary U that is independent of the input may be simulated by setting $g(t) = 0$ and choosing $H_D(t)$ appropriately.

3 The adversary method

The primary idea behind the adversary method is that if an algorithm computes a function, then it must be able to distinguish between inputs that map to different outputs. A certain amount of information about the inputs is required to distinguish them, and thus one may obtain lower bounds for the number of queries required to compute a function by upper bounding the amount of information revealed in each query.

There are several equivalent formulations of the adversary method. We describe the spectral formulation below because it is convenient. The proof below is essentially a continuous version of the proof from [HŠ05].

Consider a pair of inputs x and y such that $f(x) = 0$ and $f(y) = 1$. As above, we write $|\psi_x^t\rangle$ to denote the state of the quantum algorithm on input x at time t , and similarly for y . If the algorithm finishes after T queries, we would like $|\psi_x^T\rangle$ and $|\psi_y^T\rangle$ to be easily distinguishable, or equivalently, to have a small inner product. To distinguish the two states correctly with error probability at most ϵ , we require $|\langle\psi_x^T|\psi_y^T\rangle| \leq \epsilon'$, where $\epsilon' = 2\sqrt{\epsilon(1-\epsilon)}$. (This is known as the Ambainis output condition [BSS03].) We can use this idea to define a *progress measure* using the inner products between all pairs of inputs.

To capture the fact that some pairs of inputs are more difficult to distinguish than others, we assign a *weight* to each pair. To do so, we define a *spectral adversary matrix* Γ , which is a symmetric $2^N \times 2^N$ matrix of non-negative real values such that $\Gamma[x, y] = 0$ whenever $f(x) \neq f(y)$. (The following argument actually holds for the general adversary method, and not just for the non-negative method; see Section 5 below.) Let δ be a fixed principal eigenvector of Γ . We now define the progress measure to be

$$w^t = \sum_{x, y} \Gamma[x, y] \cdot \delta[x] \cdot \delta[y] \cdot \langle\psi_x^t|\psi_y^t\rangle$$

where $\Gamma[x, y]$ is the entry corresponding to the x^{th} row and y^{th} column of Γ , and similarly $\delta[x]$ is the x^{th} entry of δ . We also define, for $1 \leq i \leq N$, a related family of matrices

$$\Gamma_i[x, y] = \begin{cases} \Gamma[x, y] & x_i \neq y_i, \\ 0 & x_i = y_i. \end{cases}$$

Let $\tilde{Q}_2(f)$ denote the bounded-error query complexity in the Hamiltonian oracle model for f , and write $\lambda(M)$ for the spectral norm of a matrix M . The spectral version of the adversary theorem in the Hamiltonian oracle model is essentially the same as in the discrete query model.

Theorem 3.1. *For any adversary matrix Γ for f ,*

$$\tilde{Q}_2(f) = \Omega\left(\frac{\lambda(\Gamma)}{\max_j \lambda(\Gamma_j)}\right).$$

The algorithm starts in an initial state $|\psi^0\rangle$ which is independent of the input, and thus the initial value of the progress measure is

$$w^0 = \sum_{x, y} \Gamma[x, y] \cdot \delta[x] \cdot \delta[y] = \delta^T \Gamma \delta = \lambda(\Gamma).$$

To lower bound the time required for the algorithm to succeed, we upper bound the change in the progress measure. We can do this by taking its derivative with respect to time. First, note that

$$\begin{aligned} \frac{d}{dt} \langle\psi_x^t|\psi_y^t\rangle \langle\psi_y^t|\psi_x^t\rangle &= \langle\psi_x^t|\psi_y^t\rangle \left(\frac{d}{dt} \langle\psi_y^t|\psi_x^t\rangle \right) + \left(\frac{d}{dt} \langle\psi_x^t|\psi_y^t\rangle \right) \langle\psi_y^t|\psi_x^t\rangle \\ &= 2\text{Re} \left[\langle\psi_x^t|\psi_y^t\rangle \left(\langle\psi_y^t|\frac{d}{dt}|\psi_x^t\rangle + \left(\langle\psi_x^t|\frac{d}{dt}|\psi_y^t\rangle \right)^* \right) \right] \\ &= 2\text{Re} \left[-i \langle\psi_x^t|\psi_y^t\rangle \left(\langle\psi_y^t|H_x(t)|\psi_x^t\rangle - \langle\psi_y^t|H_y(t)|\psi_x^t\rangle \right) \right] \\ &= 2\text{Im} \left[\langle\psi_x^t|\psi_y^t\rangle \langle\psi_y^t|(H_x(t) - H_y(t))|\psi_x^t\rangle \right] \end{aligned}$$

Next, we can upper bound the change in the magnitude of the inner products between the algorithm

states corresponding to each pair of inputs x and y :

$$\begin{aligned}
\frac{d}{dt} |\langle \psi_x^t | \psi_y^t \rangle| &= \frac{d}{dt} \sqrt{\langle \psi_x^t | \psi_y^t \rangle \langle \psi_y^t | \psi_x^t \rangle} \\
&= \frac{1}{2 |\langle \psi_x^t | \psi_y^t \rangle|} \frac{d}{dt} \langle \psi_x^t | \psi_y^t \rangle \langle \psi_y^t | \psi_x^t \rangle \\
&= \frac{1}{|\langle \psi_x^t | \psi_y^t \rangle|} \text{Im} [\langle \psi_x^t | \psi_y^t \rangle \langle \psi_y^t | (H_x(t) - H_y(t)) | \psi_x^t \rangle] \\
&\leq |\langle \psi_y^t | (H_x(t) - H_y(t)) | \psi_x^t \rangle|
\end{aligned} \tag{1}$$

We can rewrite the difference $H_x(t) - H_y(t)$ as:

$$\begin{aligned}
H_x(t) - H_y(t) &= \{g(t)H_O(x) + H_D(t)\} - \{g(t)H_O(y) + H_D(t)\} \\
&= \sum_{j: x_j \neq y_j} g(t) (H_j^{(x_j)} - H_j^{(y_j)})
\end{aligned}$$

This shows that the progress measure w^t does not depend on the driver Hamiltonian $H_D(t)$. Now let $\Delta_j = g(t) (H_j^{(x_j)} - H_j^{(y_j)})$, and note that $\|\Delta_j\| \leq 2$ for all j . Substituting into Equation (1), we have:

$$\begin{aligned}
\frac{d}{dt} |\langle \psi_x^t | \psi_y^t \rangle| &\leq \left| \sum_{j: x_j \neq y_j} \langle \psi_y^t | P_j \Delta_j P_j | \psi_x^t \rangle \right| \\
&\leq \sum_{j: x_j \neq y_j} |\langle \psi_y^t | P_j \Delta_j P_j | \psi_x^t \rangle| \\
&\leq 2 \sum_{j: x_j \neq y_j} \|P_j | \psi_x^t \rangle\| \cdot \|P_j | \psi_y^t \rangle\|
\end{aligned}$$

Let $\beta_{x,j} = \|P_j | \psi_x^t \rangle\|$ denote the absolute value of the amplitude querying x_j at time t , and note that $\sum_j \beta_{x,j}^2 = 1$. We define an auxiliary vector $a_j[x] = \delta[x] \beta_{x,j}$ which has the property that $\sum_j |a_j|^2 = \sum_j \sum_x \delta[x]^2 \beta_{x,j}^2 = \sum_x \delta[x]^2 \sum_j \beta_{x,j}^2 = \sum_x \delta[x]^2 = 1$.

Finally, we can upper bound the derivative of the magnitude of the progress measure as follows:

$$\begin{aligned}
\frac{d}{dt} |w^t| &= \sum_{x,y} \Gamma[x,y] \cdot \delta[x] \cdot \delta[y] \cdot \left| \frac{d}{dt} \langle \psi_x^t | \psi_y^t \rangle \right| \\
&\leq 2 \sum_{x,y} \sum_j \Gamma[x,y] \cdot \delta[x] \cdot \delta[y] \cdot \beta_{x,j} \cdot \beta_{y,j} \\
&= 2 \sum_j a_j^T \Gamma_j a_j \\
&\leq 2 \sum_j \lambda(\Gamma_j) |a_j|^2 \\
&\leq 2 \max_j \lambda(\Gamma_j) \cdot \sum_j |a_j|^2 \\
&= 2 \max_j \lambda(\Gamma_j)
\end{aligned}$$

In order for the algorithm to succeed, we must have $w^T \leq \epsilon' w^0$. Since we have $w^0 = \lambda(\Gamma)$ and $\frac{d}{dt} |w^t| = 2 \max_j \lambda(\Gamma_j)$, we can integrate to obtain the theorem.

4 Comparison with the FGG proof of the lower bound for parity

When Farhi and Goldstone introduced the Hamiltonian oracle model in [FG98] and used it to prove a lower bound on a continuous-time version of Grover’s search, they referred to their technique as the “analog analogue” of the BBBV method [BBBV97]. As the discrete query adversary method is an extension of the BBBV method, the Hamiltonian oracle version of the adversary may be seen as an extension of the proof method introduced in [FG98], and indeed, it is implicit in their and Gutmann’s proof of the lower bound for the parity problem in the Hamiltonian oracle model [FGG07].

In that paper, the progress measure used is

$$\begin{aligned} |||\psi_x^t\rangle - |\psi_y^t\rangle||^2 &= (|\psi_x^t\rangle - |\psi_y^t\rangle)^* (|\psi_x^t\rangle - |\psi_y^t\rangle) \\ &= 1 - \langle\psi_x^t|\psi_y^t\rangle - \langle\psi_y^t|\psi_x^t\rangle + 1 \\ &= 2 - 2\text{Re} [\langle\psi_x^t|\psi_y^t\rangle] \end{aligned}$$

and the derivative with respect to time of this progress measure is essentially the same (up to a multiplicative factor of ± 2) of the one used in this paper.

5 Addendum: Generalising to negative weights

The argument in Section 3 actually holds for the general adversary method, and not just for the non-negative method. The non-negative method relies on the fact that an algorithm that computes a function must distinguish between inputs that map to different outputs. The general method makes explicit use of the stronger condition that any such algorithm must actually compute the function, by removing the restriction on the spectral adversary matrix Γ that its entries be real and non-negative. Even with this modification, the rate of change of the potential function, $\frac{d}{dt}|w^t|$, is still upper bounded, as above. That quantum lower bounds obtained using the general adversary method hold in the Hamiltonian oracle model follows from a version of the proof of Theorem 2 in [HLS07].

Acknowledgment

This research was done under the guidance of Richard Cleve at the Institute for Quantum Computing. The author would also like to thank Troy Lee for pointing out that the argument generalises to negative weights as described in Section 5.

References

- [Amb06] Andris Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences (JCSS)*, 72:220–238, 2006.
- [BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and Weaknesses of Quantum Computing. *SIAM Journal on Computing*, 26(3):1510–1523, 1997. Also arXiv:quant-ph/9701001.
- [BSS03] Howard Barnum, Michael Saks, and Mario Szegedy. Quantum Decision Trees and Semidefinite Programming. In *Proc. of 18th IEEE Complexity*, pages 179–193, 2003.
- [FG98] Edward Farhi and Sam Gutmann. Analog analogue of a digital quantum computation. *Physical Review A*, 57(4):2403–2406, April 1998.
- [FGG07] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A Quantum Algorithm for the Hamiltonian NAND Tree. Technical report, arXiv, February 2007.

- [HLŠ07] Peter Hoyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 526–535, San Diego, California, USA, 2007. ACM.
- [HŠ05] Peter Høyer and Robert Špalek. Lower bounds on quantum query complexity. *EATCS Bulletin*, 87:78–103, October 2005.
- [LM03] Sophie Laplante and Frederic Magniez. Lower bounds for randomized and quantum query complexity using kolmogorov arguments. Technical report, arXiv, 2003.
- [Moc07] Carlos Mochon. Hamiltonian oracles. *Physical Review A*, 75(4):042313, April 2007.
- [ŠS06] Robert Špalek and Mario Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006.
- [Zha05] Shengyu Zhang. On the power of ambainis lower bounds. *Theoretical Computer Science*, 339(2-3):241–256, 2005.